

SECTION C – PERFORMANCE WORK STATEMENT

Our technical approach is built on our team’s capabilities, cybersecurity and risk management Subject Matter Specialists, experience helping transition other agencies and building cyber-aware cultures, and proven accelerators (e.g. robust RMF, Integrated Assessment Framework, etc.). Figure 2.1-1 illustrates how our approach enables the achievement of Performance Work Statement (PWS) and agency goals and desired program outcomes.

(b) (4)



In Figure 2.1-2 on the next page, Team AT&T highlights our Phase II overview and provides a list of deliverables.

2.1 Goal 1: Proactive Audit Remediation & Management [2.1]

OCIO’s audit landscape is nuanced and complex as there are at times 15+ audits and evaluations conducted simultaneously by GAO and the OIG throughout the year, and over 220 open OCIO recommendations that date as early as 2013.

(b) (4)



OCIO requires an advisor that understands the mentality of an auditor, the audit lifecycle and governing standards (e.g., U.S. GAO – *The Green Book*), and the applicability of findings to the root challenges OCIO faces. Our relationship with GAO and OIG enables us to bring expertise through our understanding of how auditors’ approach, plan, and execute audits. This knowledge, coupled with our professional services experience, allows the Team to best support HUD in establishing effective audit readiness, internal audit support, and audit remediation capabilities.

The Team’s Audit Management Methodology offers professional skepticism, proactive collaboration with HUD and audit stakeholders, empowered executive ownership and accountability, streamlined reporting and communications, root cause analyses and prioritization efforts, and the institution of tiger teams to address risks beyond the auditor’s recommendations. Results of the Team’s efforts will be seen through the increase in accountability and preparedness of HUD, number of recommendation closures, and sustainable programs that mitigate OCIO’s priority risks.

Closure of Corrective Action Plans at BCFP

The Team supports the Consumer Financial Protection Bureau (CFPB) Technology and Innovations (T&I) Front Office under the Chief Information Officer (CIO) in managing and reporting the status of all IT related audits from GAO, OIG, Internal Controls, and Annual Independent Audits. The Team leads T&I audit coordination activities and serves as the T&I liaison in responding to over 400 provided by client requests per year. Within the first two years, the Team drove closure of over 55 Corrective Action Plans.

2.1.1 Objective 1.1: Audit Inventory Tracker [2.1.1]

The Team will leverage our Audit Management Methodology to enable HUD in tracking the full lifecycle of audit activities and to support productive and collaborative relations with GAO and OIG throughout each stage of an audit: pre-, during, and post-audit.

The Team will refine the Audit Inventory Tracker that we already built for OCIO, which is a single source of truth for audit data, to maintain progress of audit activities weekly. (b) (4)

The Team will enhance our initial tracker within 90 days of award, with subsequent weekly updates maintained in a HUD specific central repository.

The Team will execute our Audit Management Methodology, outlined in figure 2.2.1-1, to establish specialized capabilities that cover the entire audit lifecycle, enabling HUD to deploy and measure a repeatable and proactive audit management strategy. The capabilities and resulting activities for each phase of the methodology are outlined in Table 2.2.1-1 below.

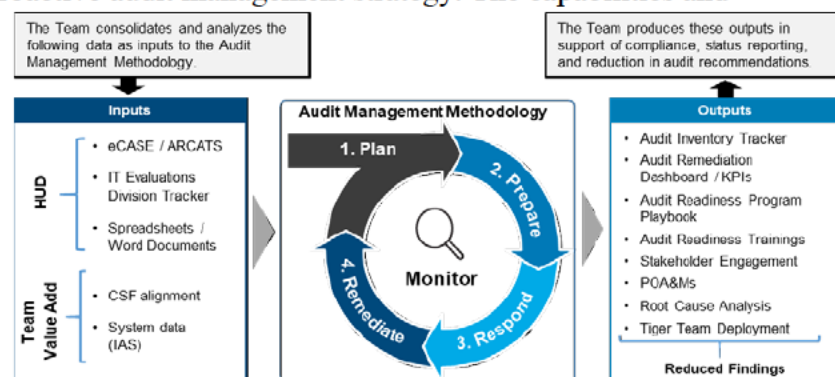


Figure 2.2.1-1

(b) (4)



The Team's revamped Audit Management Program and resulting outputs will allow for more positive Congressional hearings, which can lead to increase in OCIO budget and programmatic support. Additionally, the program will support HUD with meeting regulations and obligatory requirements, consequently reducing risk for the department.

Tiger Team Approach: The Team will bring to HUD an agile tiger team concept that aligns Subject Matter Advisors (SMAs) by units: each tiger team consists of two SMAs for three months

(b) (4) Per OCIO's approval, we will deploy the appropriate number of tiger teams based on the complexity, priority, and level of effort required to remediate the root cause of audit recommendations and risks (see figure 2.2.1-2 on the next page for the tiger team deployment strategy and example deployments). Tiger teams will collaborate with HUD to document remediation strategies and develop process documents to implement solutions compliant with HUD governance and standards (e.g., Configuration Change Management Board, Server / Database Access Request process).

Through validation of root cause, tiger teams will verify the appropriate path forward, develop POA&Ms to address the underlying risks, prepare evidence requests for closure, and support instantiation of sustainable programs. The Team will conduct periodic check points throughout the three-month deployment to track progress, address roadblocks, and forecast additional tiger team support.

(b) (4)



Dependent on the complexity and priority of audit findings and root causes, HUD will be able to request additional teams from the catalog to support or have the existing on the ground team be

deployed for a second three-month sprint. For example, a domain such as access control, which has about 35+ open audit recommendations and 35+ open ATO-related POA&Ms at HUD, may require additional teams to be deployed in comparison to a less demanding domain. Our tiger team strategy will enable HUD to implement sustainable programs and propose closure for many recommendations. The reduction in findings and recommendations will be shown through metrics 300 days from award.

2.1.2 Objective 1.2: Audit Remediation Dashboard [2.1.2]

The team will use the Audit Inventory Tracker to continue enhancing the Audit Remediation Dashboard that the Team previously built for OCIO using its analytical expertise

Figure 2.2.2-1 displays the Audit Remediation Dashboard.

(b) (4)

(b) (4)

Figure 2.2.2-1 OCIO Dashboard

The Team will tailor the Audit Remediation Dashboard to display up-to-date analytics of HUD's audit environment on a weekly basis. Weekly meetings will be held with the OCIO senior leadership team to review the dashboard, providing awareness of critical risks, issues, and overall program health. (b) (4)

2.1.3 Objective 1.3: Audit Training [2.1.3]

The Team will document and communicate audit roles and responsibilities through a persona-driven approach. We will engage with OCIO stakeholders proactively throughout the audit lifecycle by implementing a strategy that addresses needs of each of the four key stakeholder groups: Executive Leadership, Management, Process and System Owners and Audit Liaisons. We will provide two in-person/web audit readiness trainings per stakeholder group and up to ten ad-hoc trainings for new stakeholders using the defined roles to educate them on their responsibilities and the audit process (refer to the Cyber Training and Awareness Plan (Objective 4.3)). This training will show stakeholders how and when to engage with auditors, the do's and don'ts of the audit process, and proactive fulfillment their responsibilities proactively.

(b) (4)

A large rectangular area of the document is completely redacted with a solid black fill.

Ultimately, the Team's Audit Management Methodology will enable proactive stakeholder engagement, increase productivity and accountability, provide visibility into audit activities and status, reduce audit recommendations, and implement sustainable programs.

2.1.4 Objective 1.4: Update Cyber Program Roadmap [2.1.4]

We will provide updates to HUD's existing Cyber Program Roadmap as outlined in Objective 4.5: Update Cyber Program Roadmap. Below is a figure of our goal 1 proactive audit remediation and management schedule, deliverables, and a table of performance results.

(b) (4)

A large rectangular area of the document is completely redacted with a solid black fill.

Figure 2.2.4-1 Goal 1: Proactive Audit Remediation and Management

(b) (4)

A large rectangular area of the document is completely redacted with a solid black fill.

(b) (4)



(b) (4)



2.2 Goal 2: Cyber Governance and Risk Management System [2.2]

Organizations have challenges balancing the need to maintain compliance with regulations and the desire to modernize. The Team will support HUD's ongoing compliance and modernization efforts by establishing a cyber governance structure to update HUD's cyber control catalog, risk categorization methodology, and develop/update policies, processes, and methodologies.

2.2.1 Objective 2.1: Risk Management Framework [2.2.1]

We will develop a Policy Working Group, a formal establishment of cyber decision makers that will inform the direction of policy decisions and contextualize security requirements with HUD's business processes. Activities include:

- Facilitate up to 12 monthly Policy Working Group meetings to gather requirements for HUD's cyber policies, processes, and methodologies.
- Document and disseminate decisions from the Policy Working Group, and adjudicate requirements into appropriate policies, processes, and methodologies.

In addition, we will create or update up to (b) (4) such as: Authorization Policy, Creating and Managing POA&Ms, Vulnerability Management Policy, IT Security Policy Handbook, Risk Categorization Methodology. The Team will develop policies based on a stakeholder-focused approach to increase adoption rates across Program Areas. These policies will serve as the foundation for HUD's risk management program and will enforce the organization's compliance to continuous monitoring and ongoing authorization activities.


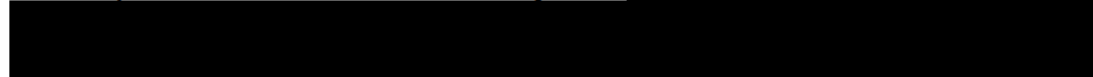
2.2.2 Objective 2.2: Cyber Control Catalog [2.2.2]

The Team will provide HUD with a customized cyber control catalog and risk categorization methodology (180 days after award) to help the organization define its security control requirements and prioritize remediation actions to high impact systems. We will evaluate HUD's cyber control catalog and risk categorization methodology, and will achieve this by:

(b) (4)



Through the analysis of HUD's cyber control catalog and risk categorization methodology, we will work with the Policy Working Group to determine key risk-reducing controls to implement across up to 55 HVAs/Mission-Critical systems (b) (4)

2.2.3 Objective 2.3 Update Cyber Program Roadmap [2.2.3]

We will provide updates to HUD's existing Cyber Program Roadmap as outlined in Objective 4.5: Update Cyber Program Roadmap. Below is a figure of our goal 2 cyber governance and risk management system schedule and deliverables and a table of our measure of performance and success.

(b) (4)



2.3 Goal 3: Security Operations Center (SOC) Deployment Plan & Operating Model [2.3]

The AT&T Team offers HUD a security operations solution that meets Federal Government FISMA Standards, within a hardened facility, and leverages 50 years of experience delivering security operations for Federal and commercial customers. The Team will provide HUD with a mature detection and response capability designed to mitigate against threats that put HUD's most critical assets at risk. We will accomplish this by providing a high-performing team, executing process discipline, and optimizing the use of security technologies.

2.3.1 Objective 3.1: SOC Deployment Plan & Operating Model [2.3.1]

The AT&T Team will develop a SOC deployment plan and operating model addressing people, process, and technology as well as physical and logical infrastructure required for enabling the SOC. The Team will document the approach, timeline, and resources required to establish a fully developed HUD SOC capability within the Chief Information Officer (CIO) organization that leverages AT&T's SOC managed service to satisfy the Threat Management capability.

The Team will develop an integrated SOC operating model consisting of five functional capabilities, supported by an operational governance model to ensure effective synchronization between our managed service and the HUD cybersecurity staff

(b) (4)



The Team will document our deployment plan and operating model detailing the following:

- Introduction
- Purpose
- Team structure, integration model, roles and responsibilities
- Deployment plan
- Schedule (Key milestones and deliverables)
- SOC Metrics/KPIs
- SOC optimization processes
- Event alert prioritization and reporting processes
- Attack Surface Reduction Processes
- Threat Intelligence processes
- Incident Response (IR) processes
- Playbook integration

The Team will incorporate system architecture, integration with technology, and engineering of the SOC monitoring function.

(b) (4)




The Team will systematically increase Threat Monitoring visibility throughout the network enterprise through an incremental security log data integration approach and the deployment of a consolidated Splunk SIEM.

(b) (4)

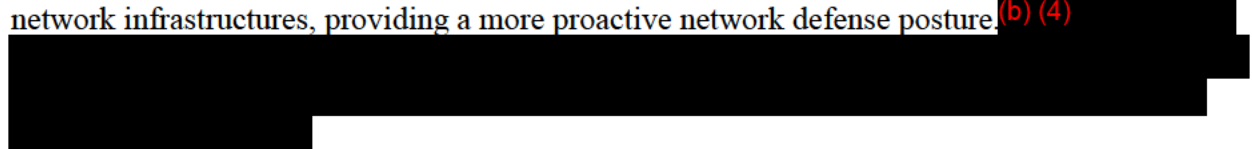


The Team will purpose build operational process improvements tailored to HUD's unique requirements to ensure synchronized and efficient security operations throughout HUDs cybersecurity organization. (b) (4)



The Team will develop and deliver an Incident Response Plan that is aligned with National Incident Management System (NIMS) and is NIST compliant. The purpose of this plan is to make incident response consistent for all potential types of incidents. NIMS and NIST compliance enhance the scalability of the framework, allowing interaction with local, state, and federal resources using common methods and terminology defined at the federal level.

The Team will utilize multiple threat intelligence sources that consist of open source, subscription-based, and other commercial subscription services to inform HUD's SOC technology and provide operational cyber threat reports to the HUD Threat Intelligence team and their leadership. The solution enables the discovery, analysis, and visualization of previously hidden relationships within vast collections of data at petabyte scale. These discoveries will be used to identify, respond to, and / or mitigate vulnerabilities to HUDs, systems, platforms, and network infrastructures, providing a more proactive network defense posture. (b) (4)




2.3.2 Objective 3.2: SOC Use Cases & Splunk Deployment / Tuning [2.3.2]

(b) (4)



The Team will normalize HUD's security log data to align to Splunk's Common Information Model (CIM) to support the consistent, normalized treatment of data for maximum efficiency when developing reports, correlation searches, and dashboards to present a unified view of HUD's security domain. (b) (4)



(b) (4)



(b) (4)



2.3.4 Objective 3.4: Update Cyber Program Roadmap [2.3.4]

We will provide updates to HUD's existing Cyber Program Roadmap as outlined in Objective 4.5: Update Cyber Program Roadmap. Below is a figure showing our SOC deployment and

operation model schedule and deliverables and a table outlining our measures of performance and success.

(b) (4)



2.4 Goal 4: Cyber Strategy and Innovation [2.4]

To advance HUD's cyber maturity and formalize the cyber program, OCIO must have a focused strategy, facilitate awareness and innovation, and execute activities in accordance with the OCIO Cyber Roadmap. The Team will develop an end-to-end strategy that establishes a strong foundation for strengthening HUD's reputation as a business enabler, identifies high-risk data elements, and develop a plan for securing them.

2.4.1 Objective 4.1: Cyber Strategy [2.4.1]

An important component of our strategy implementation is defining an organization's ideal state of operation and performance, using it as a guide to set goals, identify priorities, and mitigate roadblocks to advance maturity.

We will develop a **Cyber Vision and Mission Statement** as the foundation for HUD OCIO's overarching strategy by designing and executing a series of ideation workshops with select

stakeholders and evaluate the current state of the organization through stakeholder interviews, focus groups, and surveys to identify and prioritize improvement areas for a successful transformation. The Team will communicate to stakeholders and work with HUD OCIO leadership to establish personal commitments on how individuals will reinforce and demonstrate the organization's vision and mission statement

(b) (4)



HUD must determine which data and systems should be prioritized and protected. The Team will identify and categorize high-risk data elements based on business criticality and sensitivity. We will develop and distribute questionnaires and conduct interviews to gather inputs from the program offices. Once we gain an understanding of high-risk data elements, we will perform an analysis of HUD's capabilities in protecting that data throughout its lifecycle (i.e., acquisition, use, storage, sharing, retention). We will integrate industry leading data protection technologies (i.e., data classification, data loss prevention, digital rights management, etc.) into our recommendations and prioritize them based on feasibility and impact.

2.4.2 Objective 4.2: Cyber Innovation Evaluation Process [2.4.2]

HUD needs an effective process to evaluate emerging cyber innovation and technologies and their integration into the agency. The Team will use our Federal IT Project and Portfolio Management Framework to build a process that considers people, processes, and existing technology to minimize risks and maximize returns associated with innovation. In doing so, we will:

(b) (4)



(b) (4)



2.4.3 Objective 4.3: Training & Awareness Plan [2.4.3]

An essential element of cyber transformation involves stakeholders to operationalize programmatic changes into day-to-day activities. The Team will train HUD stakeholders and establish clear and regular communications, elevating the department's understanding of cyber best practices, policies, and procedures. We will:

(b) (4)



We will also develop specialized security trainings by creating specific roles, or “cyber personas” that reflect the segments of the workforce and outline the specific cyber risks associated with each role. The personas will serve as the basis for the specialized security trainings. The sample personas outlined in figure 2.5.3-1 below are based on our experience delivering a role-based approach to cybersecurity awareness and training with other federal

(b) (4)



Figure 2.5.3-1 Sample Personas

Figure 2.5.3-2 Analyze, Design, Develop, Implement, Evaluate (ADDIE) model

The Team will deliver virtual and in-person role-based trainings, enhanced content, and immersive learning opportunities, such as: gamification, interactive video, and simulation exercises for each persona where appropriate to maximize engagement and participation. Finally, we will leverage NIST's National Initiative for Cybersecurity Education (NICE) Workforce Management Working Group to help OCIO integrate a persona-driven training and awareness effort that builds on the existing program and can be replicated and scaled as needed.

2.4.4 Objective 4.4: Dashboard & Reporting [2.4.4]

HUD needs an overarching reporting capability containing contextualized metrics that inform, educate, and enable stakeholders to make decisions. We will develop a Cyber Dashboard that tracks program implementation and risks. We will follow our design, implement, and operate methodology, described in figure 2.5.4-1 to develop the cyber dashboard and establish a programmatic reporting capability that:

(b) (4)



Figure 2.5.4-1 Cyber Risk Dashboard & Reporting

A reliable reporting capability will enable HUD to measure progress against various information security goals as the organization undergoes widespread IT modernization and program enhancements.

2.4.5 Objective 4.5: Update Cyber Program Roadmap [2.4.5]

We will work closely with all Cyber Program work streams to collect, organize, and update data gathered in Year One to strengthen HUD's current cybersecurity posture and enable HUD to achieve a comprehensive Cyber Program. Below is a figure showing our cyber strategy and innovation and a table highlighting our measure of performance and success.

(b) (4)



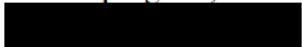
(b) (4)



2.5 Goal 5: Continuous Monitoring [2.5]

The Team's RMF solution and past performance across the federal government demonstrates we have proven experience changing the way that cybersecurity programs are implemented. Our philosophy is to balance compliance requirements with drivers of HUD's business success, allowing Program Areas to make decisions about applying cybersecurity to support the mission.

2.5.1 Objective 5.1: Establish and Develop an Authorization Requirement [2.5.1]

As depicted in Figure 2.6.1-1 on the next page, we understand that all information systems must receive its Authorization to Operate (ATO) to establish an ongoing authorization program, and the Team will perform a zero-base review of HUD's information systems 
We will complete this activity by:

(b) (4)



(b) (4)



(b) (4)

We will do this by facilitating guided workshops to determine the organization's risk tolerance, varying risk thresholds, and cadences for event-driven and time-driven briefings to prompt the appropriate authorization actions, specifically prioritizing the ongoing authorization activities of HUD's GSS and Major Applications.

2.5.2 Objective 5.2: Implementation of Continuous Monitoring and Authorization [2.5.2]

Continuous monitoring data and security reporting/dashboarding are the vehicles that allow for SOs and AOs to make informed decisions regarding the risk posture of information systems based on updated/refreshed data, enabling the organization to enter a state of ongoing authorization. The Team will help HUD execute continuous monitoring and ongoing authorization activities (b) (4)

The Team will maintain the continuous monitoring schedule and assess security controls for authorized systems. We will provide guidance and recommendations for the assessments we conduct, including: determination if a re-authorization is recommended, the most efficient assessment type based upon system changes (e.g., applying a System Impact Analysis (SIA) or automated assessment to instead of a full-scope assessment), and security assessment results including the findings identified in the assessments.

We will implement ongoing authorization reporting and metrics at HU by:

(b) (4)

(b) (4)

Our approach will help HUD build a cybersecurity risk management program that better identifies, contextualizes, and correlates data to facilitate decision making. By aligning risk management activities with organizational risk tolerance and business needs, we will enable HUD to implement risk management in a cost-effective and strategic manner.

2.6.3 Objective 5.3: Update Cyber Program Roadmap [2.3.4]

We will provide updates to HUD's existing Cyber Program Roadmap as outlined in Objective 4.5: Update Cyber Program Roadmap. Below is a figure of our goal 5 schedule and deliverables and a table of our measure of performance and success.

(b) (4)



(b) (4)



(b) (4)



(b) (4)

